Box 8275
G-4-A
9-4
ARB

~~TOP SECRET "U"~~ TICOM/I-176

HOMEWORK BY WACHTMEISTER DR. OTTO BUGGISCH
OF OKH/CHI AND OKW/CHI

Attached in a translation of a report, based on questions supplied by us, written by Wm. Dr. BUGGISCH, of OKH/Chi and OKW/Chi, at P/W Camp A 21 during November, 1945.

The report was received from S.I.D., USFET.

Previous homework by BUGGISCH has been issued as TICOM/I-72 and I-137.

5771

Trans: A.C.J. Copy No. 9

No. of Pages: 13

TICOM

17th December, 1945.

DISTRIBUTION

British

1. D.D.3.
2. H.C.G.
3. D.D.(M.W.)
4. D.D.(A.S.)
5. C.C.R.
6. Cdr. Tandy
7. Major Morgan

U.S.

8-11. Op 20-G (4) (via Lt. Cdr. Manson)
12. G-2 (via Lt. Col. Hilles)
13-16. A.S.A. (4) (via Capt. Collins)
17. Director, S.I.D. USFET
18. Col. Kankel, USAAFE

TICOM

19-21. S.A.C. (3)
22. Cdr. Bacon
23. Lt. Cdr. Manson
24. Major Cowan
25. Capt Collins
26-29. Ticom Files (4)

Additional

30-32. Mr. Pritchard (3)
33. Mr. R. R. Jackson
34. Mr. Twinn
35. Mr. Bonsall

Approved for Release by NSA on 07-25-2017, FOIA Case # {66109}

RECORD COPY
DO NOT DESTROY OR MUTILATE
Copy No. 1
2-4836
FHV

Doc ID: 6587330

NSA25X3

Dr.Otto BUDGISCH
PW Camp A 21.

Darmstadt, 1.11.45

1) What do the designations F90 and F110 refer to? If these are cryptographic systems, give description of systems and method of solution. By whom were they used?

F90 and F110 were German designations for French Army cipher systems before and during the campaign in FRANCE. Both were based on a four figure code, in one case the recipher consisted of a periodic adder [or subtractor] of length 11; in the other it was ordinary transposition, the transposition key being obtained from a key word which itself was taken from the code and shown by an indicator group. Both systems were being read from the winter of 39/40 to the end of the French campaign. Solution was by methods generally known in cryptanalytic circles. One of the codes turned up again for a short period in De Gaullist traffic.

5771

2) Describe the organisation of In 7/VI and the functions of its subdivisions, including an administrative diagram.

At my interrogation on 25th August Major BUNDY showed me fairly complete plans of the organisation of In 7/VI or Ag N/NA, which contained considerably more detail than I myself was able to remember. At that time I could only give a few quite insignificant additional facts.

3) What is OK 40? Describe system and method of solution. By whom used ?

OK 40 is the official Russian designation for a Russian 5/F code (operational code, ОПЕРАТИВНЫЙ КОД 40). It contained 25,000 groups namely all the five figure numbers, and only these, in which the first three figures are all simultaneously odd or simultaneously even. For reciphering the adder [subtractor] of 300 5/F groups in general use by the Russians was used. The code was used from about the end of June to September '41 by the higher and highest Russian commands (naturally only in the army, not by NKVD units). Soon after the beginning of the Russian campaign several copies of the code were captured; we also frequently came across recipher tables, most of which however were out of date, as even at that time the Russians were changing them frequently, even though they had not yet begun changing them daily invariably. Owing to the already mentioned special characteristic of the first three elements of the code groups it was particularly easy to line them up. In this way depths of 8-12 were often obtained, so that the recipher could easily be stripped by well known methods. Detailed information on this and similar Russian systems is contained in the report submitted to USFET Intelligence service in July '45 by my then fellow prisoners DETTMANN and SAMSONOV, with whom I had worked during the summer of '44 on breaking the system.

Doc ID: 6587330

4) What was the swiss machine messages mentioned? What was the method of solution?

These were messages of the Swiss Confederate Army (probably practice messages without operational content) which were probably enciphered on an Enigma Model K. At that time I worked out a theoretical method of solution only, which also gave successful results in practice on trial texts enciphered by myself, but which however could not be applied to the Swiss messages as the internal wiring of the Swiss wheels was not known. The method is too lengthy to be explained in a few lines, moreover I should need some little time and assistance to reconstruct it, as the details have escaped my memory.

5) (1) What was the B 211 method developed by Dr. Von DENFFER and HILBURG, and completed by BUGGISCH? Did it apply to the ordinary commercial B 211 or to the modified French model described by BUGGISCH? Give the method in detail

(2) Did BUGGISCH have any theory about the failure of the B 211 messages to decode according to the method worked out?

(3) A K-37 was captured from the Germans which has plugs on each side of the commutators leading to some mechanism which is missing. Does BUGGISCH know this machine? If so, what is the missing mechanism? What was the method of solution mentioned? Which way did the current go through the comautator?

(4) Exactly how did K-37 differ from B 211? Can BUGGISCH give more details than before?

I myself have not worked on the Russian K 37 nor the French B 211, as is assumed to be the case in question 5 ("completed by BUGGISCH"). My special investigations in the field of cipher machines were concerned either with "Hagelin Typ kleine Technik" (C 36, BC 38, machine 41) or with the Enigma type (Model K, Army and Navy systems, machine 39), but never with the quite different type "Hagelin Typ grosse Technik" (B 211 and K 37). I have only a quite superficial knowledge of this type, based on occasional hints by Dr. Von DENFFER, who told me about his investigations in quite general terms from time to time. All that I know about it is contained in the following:

I first learned of the existance of the French machine in the Autumn of '40 in BERLIN. I was told (possibly by Ob.Insp. KÜHN ?) that a Wachtmeister (later Leutnant) BÜRKLIN, of whom the then Head of the Cryptanalytic Section, Major JUNG, had a very high opinion, had taken to pieces a captured "large" French cipher machine (of a type quite different from the C 36 known to me), but had not been able to put it together again. There were as far as I know no investigations concerning it made at that time by members of the Horchleitstelle or of In 7.

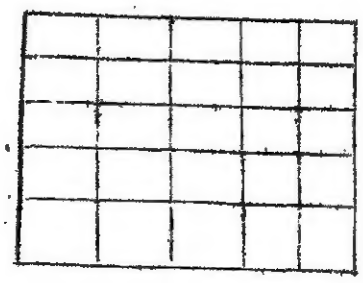
Doc ID: 6587330

During the year '40 or '41 a few more captured machines must have arrived in BERLIN, but it could not have been until '42 that I saw some of them myself for the first time. They were quite incapable of being made to work, and I was too busy with other things to bother about them, and in any case had no instructions to do so.

The cryptanalytic analysis of the type "Grosse Technik" did not begin in connection with these machines, but with the capture of a model of the Russian machine K 37. This arrived at LÖTZEN at the end of June or beginning of July '41 and was at once investigated by DENFFER and HILBURG, who however had no inkling of its relationship with the French B 211, which they probably at that time knew only by name.

The cryptographic principle of the captured Russian machine, which had the designation "K 37" marked on its case, is as far as I know the following: the letters of the alphabet (omitting infrequent letters) were entered in a square of 5 x 5 = 25 squares:

Q =



To the nth keying (n = 1,2,3, ...) there correspond two permutations of the 5th order:

$$Z_n = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \alpha_1^{(n)} & \alpha_2^{(n)} & \alpha_3^{(n)} & \alpha_4^{(n)} & \alpha_5^{(n)} \end{pmatrix} = \text{"row permutation"}$$

$$S_n = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \beta_1^{(n)} & \beta_2^{(n)} & \beta_3^{(n)} & \beta_4^{(n)} & \beta_5^{(n)} \end{pmatrix} = \text{"column permutation".}$$

If the nth letter of clear text is in the K-th row and the λ-th column of the letter square Q, the corresponding cipher letter is determined as the intersection of row $\alpha_k^{(n)}$ and column $\beta_\lambda^{(n)}$. The dependence of the permutations Z_n and S_n on n is regulated by two relatively simple systems of pin wheels, the construction of which is the same in the B 211; however I no longer remember the details. The K 37 has in addition 2 systems each of 5 plugs which bring about additional permutations A of the rows and B of the columns. Probably each of these pluggings was traversed only once, i.e. probably the effective row and column permutations were

AZ_n and BS_n respectively, and not
$AZ_n A^{-1}$ and $BS_n B^{-1}$

Doc ID: 6587330

However I am no longer certain of this, after over 4 years. At all events there was no difference from the French B 211 in this respect also, as was shown by a later comparison of the machines. The Russian machines had no further complications. The method of solution depended on dragging a word of 9 or more letters. At that time the word ПРОТИВНИК was found particularly suitable, as it headed the list in the frequency statistics of words of 9 or more letters in the messages read up to that time (5/F material). Trial Russian messages enciphered with the captured machine could be perfectly deciphered by the method of solution developed, however it was never put to practical use, as the German intercept stations never intercepted messages which could be assumed to have been enciphered with the K 37. Also as far as I know no other example of this or of any other Russian cipher machine was captured.

In the late autumn of 1941 Von DENFFER and HILBURG in BERLIN established that the K 37 corresponds exactly to the French B 211 in fundamental cryptographic principle, only in the French machine a further reciphering device (French "surchiffreur") is added; its working in detail is not known to me; I can only remember the following:

a) Among other things the "surchiffreur" contains a wheel of type similar to an Enigma wheel,
b) there were two different types of wiring the machine with the "surchiffreur": parallel, and crossed;
c) the "surchiffreur" influenced the pin wheels mentioned in the above description so that the actual movement of these was more complicated in the B 211 than in the K 37.

While I am fairly certain of the statements in a) and b), I may be wrong regarding c); in any case too great importance should not be attached to statement c). Although the B 211 appeared to be considerably more complicated from the cryptographic point of view than the K 37, Von DENFFER and HILBURG succeeded in the winter of 41/42 in generalising the system used for the K 37 to such an extent that at least in the case of parallel wiring a practical solution could be effected. Thereby it was found possible to break old French original messages from the year 1940 for which no keys had been captured. For crossed wiring the method of solution probably became somewhat longer, but could still be carried out. As to the reasons why these methods of solution were not successful later, when B 211 messages turned up in De Gaullist traffic, only conjectures were offered. The simplest assumption was that the fundamental square Q had been altered. In any case no message from De Gaullist FRANCE was ever deciphered, as far as I know.

6) Was the strip system solved in 1942 used by the Military or was it diplomatic traffic? By what U.S. agencies was the strip system used which was solved at In 7/VI in 1942?

I myself never worked on the strip system and hence do not know the senders, recipients and message contents. However I think I once heard offhand that OKW/Chi were also reading it in addition to my own unit In 7/VI. Accordingly it is probable that both military and diplomatic texts were being read by the Germans.

Doc ID: 6587330

7) Who was Dipl. Ing. VOSS and what was his function at STOCKHOLM?

VOSS was at Wa A Prüf 7/IV as a qualified engineer in Dr. PUPP's section, and in 1941 (?) purchased two commercial models of the BC 38 from the firm Kryptotechnik in STOCKHOLM on behalf of this section. His being in a reserved occupation was later cancelled, he went into the army and went to some specialist unit or other.

8) What were the "results of the Forschungsamt "mentioned in connection with Russian cypher teleprinter?

The FA [Forschungsamt] had analysed a Russian cipher teleprinter system in 1943 and recognised that it must have been based on a machine having certain similarities with the German SZ 40. After a short time the Russians altered the system. The FA then communicated its results to my unit and was given as a kind of recompense a report on the solution of a German cipher teleprinter. This was one of the very rare cases where FA and In 7/VI exchanged results. I did not study the FA results at that time, as I was not responsible for work on cipher teleprinters, and hence can give no details. At all events the Russian machine (just as in the German types SZ 40, SF 42, but in contrast to T 52 a,b,c and d) gave only 32 different substitution alphabets, the succession of which became periodic only after an astronomically large number of steps. This succession was given by a system of pin wheels, the peripheries of which were prime to each other and at an estimate lay between 30 and 90. In any case there was no complicated mutual influence of the pin wheels on each other (as for example in the T 52 d).

9) Give first names,physical descriptions, home addresses, and estimate ability of the following persons previously mentioned: (Names given in answer below).

The personal data are given according to the following pro-forma:

a) name
b) Christian name
c) military rank and service appointment where appropriate
d) civil occupation, or whether officer or army official by profession before the war
e) last place of residence known to me
f) ability, distinguishing between the following types:

A_1) Expert cryptanalyst
A_2) Very good cryptanalyst
A_3) Moderate cryptanalyst
A_4) Only a few fundamental ideas about cryptanalysis
A_5) No cryptanalytic knowledge
B_1) An efficient officer in general also a good unit commander; knowledge in the sphere of signals recce (various forms of evaluation, operation of signals recce units etc.); good to very good organiser; in my personal opinion well fitted for the position held as Section Head etc.,in the OKH.

Doc ID: 6587330

B_2) As an officer in general not particularly outstanding; some knowledge of signals recce, moderate organising ability; in my personal opinion unsuitable for the position held as Section Head etc.

C_1) Efficient qualified electro-technical engineer (for example HF and long distance communications technique).

C_2) Qualified electro-technical engineer with only moderate theoretical and practical knowledge.

METTIG, b? Major and Section Head, professional officer, BERLIN, UHLANDSTR or in the neighbourhood, A_4 B_1.

FRANZ, b? Major (or Obstlt.?) and Kommandeur der NA (?), professional officer, BERLIN?, A_4 or A_5, B_2.

KÜHN, OTTOKAR, Oberinspektor, Heeresbeamter, JÜTERBOG, A_2.

WOLLMANN, Oberst, dead.

MÜLLBECK, b?, Hptm, d?, e?, A_4, B_2.

HÜTTENHAIN, b?, Regierungsrat, Dr., permanent civil servant at OKW/Chi (formerly an astronomer), BERLIN, A_1.

MENZER, b?, Ob.Insp., Heeresbeamter, BERLIN, A_1 (at least as a practical man working by intuition; no comprehensive theoretical knowledge).

BLESCHKE, MAX, Sdf.(K), permanent civil servant of OKH, BERLIN, A_2 for Soviet RUSSIA, otherwise only A_3.

DETTMANN, ALEX, Leutnant, permanent civil servant of OKH, LÜBECK (at present a fellow prisoner with me at USFET Intell. Serv.), A_1 for RUSSIA only.

TORUNSKY, b?, Inspektor (?), permanent civil servant of OKH, e?, in Russian field A_2 - A_1 (?).

LIEDTKE, ?, Ob.Insp., Heeresbeamter, e?, A_1 (no mathematical or theoretical knowledge, a purely intuitive worker, but as such specially outstanding, particularly for hand systems. In my opinion not so well suited for work on machines, for example).

Doc ID: 6587330

KETTLER, ?, Oberst and Abteilungschef of Chi professional officer, BERLIN (or SILESIA ?) A_5, B_1.

JUNG, b?, Major, professional officer, e?, A_3.

BAILVIC, b?, Ob.Regierungsrat, Heeresbeamter, JÜTERBOG - BERLIN - VIENNA, A_3 (must have been formerly a very good cryptanalytic but has taken no active part in cryptanalytic work in recent years for reasons of age and preoccupation with purely administrative work), B_1.

HASSEL, b?, Oberst and Amtsgruppenchef of In 7, deprived of his office in connection with the 20th of July 1944 and transferred to NORWAY, supposed to have been afterwards arrested there by the Gestapo (??), professional officer, BERLIN (??), A_4 B_1 (purely military type with little understanding of the special nature of cryptanalytic work).

MANG, b?, Obstlt and Kommandeur NA, professional officer (?), VIENNA (?), A_4 B_2.

KUNZE, ?, civilian, Ob.Reg.Rat and Head of the Mathematical - Analytical Cryptanalytic Section in the Foreign Office, A_1.

DÖRING, HEINRICH, Wachtmeister, Dr., mathematician, JÜTERBOG, A_1.

v. DENFFER, HERBERT, Leutnant, Dr., mathematician, JÜTERBOG, BERLIN or near STETTIN, A_1.

HILBURG, FRITZ, Wachtmeister, mathematician, JÜTERBOG/BERLIN, A_1.

PUPP, b?, civilian and Referent with Wa Prüf 7/IV, Dr. Ing., BERLIN, C_1 A_5.

VOSS, b?, Gefreiter (?), qualified engineer, BERLIN, A_5, C_1.

LUZINS, PETER, Uffz., Dr., mathematician, JÜTERBOG/BERLIN, A_1.

KOCHENDORFFER, b?, Gefr (?), Dr., mathematician, e?, A_1.

STEIN, b?, Leutnant, Dr., mathematician, BERLIN, A_1.

HASENJÄGER, b?, Ob.Leutn., mathematical student, BERLIN, A_1.

TRÖBLIGER, b?, Uffz., mathematician, BERLIN-FROHNAU or a town in the Palatinate (?), A_2.

BEEGEMANN, b?, Kapitän z.See and Abt.Chef (?) OKM Skl MND, professional officer, BERLIN ?, ??.

SINGER, b?, Fregattenkapitän and Section Head (?) OKM Skl MND, professional officer, BERLIN (?), A_3 (?), C_1 (?).

Doc ID: 6587330

WEIDEMANN, b?, Obstlt. and Section Head Wa Prüf 7/IV, professional officer, BERLIN-ANSBACH (BAVARIA), was released from Dispersal Camp on 15.6.45, probably in the neighbourhood of ANSBACH, A_5 B_2 C_2.

LOTZE, HERBERT, civilian, Dr. Ing., STAATS near STENDAL, A_4 C_1.

VIEGEMUND ?

SCHONE, HERMANN, civilian, qualified engineer, STAATS near STENDAL, A_4 C_1.

KERKHOFF, ?, Oberbaurat, Heeresbeamter, VELTEN near BERLIN (?), A_4 or A_5, C_1.

GÖING, b?, civilian, Dr. Ing., Ebermanstadt, C_1.

GRAMBERG, KURT, Obergefreiter, Dipl. Ing., MISDROY, A_2 in special Russian sphere (special employment in listening to X2 traffic).

FRICKE, b?, Sdf (Z), Dr., astronomer, BERLIN BABELSBERG (observatory), A_1.

VAUCK, b?, Ob.Leutn., Dr., Studienrat in mathematics, DRESDEN A_2 - A_1.

PIETSCH, b?, Reg. Baurat, Dr., mathematician, JÜTERBOG, A_1.

RADEMACHER, dead.

SAMSONOV, SERGINS, Wachtmeister, at present a prisoner with me at USFET Intelligence Service, business man, HAMBURG, in special Russian sphere A.

KRANT, b?, Uffz., Dipl. Ing., e?, A_2 for RUSSIA.

PAECHTER, b?, Obstlt. and Section Head of Wa Prüf 7/III, professional officer, e?, A_5, B_2 ? and C_2 ??

ZSCHOCHE, b?, Major and deputy Section Head of Prüf 7/IV, professional officer (?), BERLIN ?, A_5 ??

BRETSCHNEIDER, b?, Sdf (K), Dipl.Ing., DRESDEN or CHEMNITZ (?), C_1.

LINDMEIER, FRIEDRICH, Uffz., Dr., mathematician, VIENNA, A_2.

PORT, b?, Hauptmann (Luftwaffe), professional officer (?), ?, A_3 or A_4.

HOHEISEL, GUIDO. Reg.Rat, professor in ordinary of mathematics at COLOGNE University, A_3 or A_2 (in cryptanalysis only since Autumn of '44).

Doc ID: 6587330

STEINBERG, b? Reg.Baurat, mathematician, BERLIN, A_2.

BOEHM, b?, ?, mathematician, A_1 or A_2 ??

RINOW, b?, Uffz., Lecturer in Mathematics, Dr. habil. BERLIN University, A_2.

WÜNSCHE, b?, Gefr., Dr., mathematician, BERLIN TEMPELHOF, A2.

LÜDERS, DAVID, Ob. Leutn., mathematical student, JÜTERBOG - LEIPZIG, A_2.

JESSE, b?, Uffz, Studienrat Math., BERLIN REINICKENDORF, A_2.

FRIEDE, GEORG, Wachtm., Dr., mathematician, GÖRLITZ, A_2.

FOPPL, b?, Uffz., chemical student, MUNICH, A_2.

VALENTIN, WERNER, Wachtm., Studienrat for mathematics, BEESKOW, A_1.

LACHNER, b?, Uffz., qualified engineer, VIENNA, A_2.

10. We have heard that LACHNER was engaged in Work on American cypher teleprinter traffic. Give details of this.

I do not know of any results on American cipher teleprinter messages. As long as I was working at Ag N/NA , the incoming message material was only being collected together. If LACHNER worked on it, it must have been after June '44. It appears improbable to me that any results have been achieved in this field.

11) Are designations OK 40 and K 37 German?

Both are Russian designations. Cf. 3) and 5).

12) What were the mentioned Enigma and Typex documents at MATTEIKIRCHPLATZ ?

I was interrogated in July in REVIN by Major BUNDY and two officers (captains) of the English Intelligence Service (sic) about this and subsequently wrote a detailed report on it, at least as far as Type X was concerned. The written report was concerned with theoretical investigations by mathematicians of In 7, also about English material captured at DUNKIRK.

13) What matters were dealt with at Chi conferences held in BERLIN at instigation of General GIMMLER in 1944?

The purpose of the Chi conferences was to obtain unity among all German authorities using cipher systems (OKW, Army, Navy, Luftwaffe, Foreign Office, Reichsbahn etc; strangely enough, the police and the SS were not represented) as to the judgement on the security of these systems.

Doc ID: 6587330

About 5-7 of these conferences took place, I myself being present at only three of them. The first one was about September 44; then there were several during October and November (or possibly the beginning of December) and lastly there was a final one on the 24th of January 1945. This was different from the other ones firstly in that the number of participants was much larger (about 40 officers etc.) and secondly that instead of considering and criticising an already existing German cipher system, as had been the case before, the members of the conference were in three lectures given a survey on general lines of speech encipherment, which was to the majority of them entirely new. At the conferences in 1944, on the other hand, only a small group of specialists met on each occasion, and hand ciphers, cipher machines and cipher teleprinters used by various German authorities were considered with regard to their security and the use of insufficiently secure systems was forbidden. I myself took part in two conferences on the Enigma (Army model, Navy model, model K, model G). K and G machines were declared to be not sufficiently secure; the Reichsbahn was to be forbidden to use the K machine any more. The Army and Navy Enigmas appeared to be sufficiently secure for practical use provided that the regulations were rigorously adhered to - even though from a theoretical standpoint there were misgivings about these machines. The Naval emergency cypher was declared insecure and was to be replaced by a better one.

14) What is the history of the "Fall WICHER"?

In the autumn of '39 a rumour that the Poles had been reading the German Army Enigma reached the German cipher authorities. This was occasioned by the capture in 1939 of Polish secret documents containing clear texts of German cipher messages. I believe that several persons in subordinate positions in the WARSAW Cryptanalytic Service were arrested after the Polish campaign, but were released after a short time without our being able to learn any details. Among other things the list of salaries of members of the Cryptanalytic Bureau was found, according to which two mathematical students from POSEN received particularly large salaries, which led to the somewhat vague supposition that they had perhaps deciphered the Enigma messages. Neither of them could be found. Soon after this our people calmed down again. At the beginning of '40 theoretical investigations by several mathematicians of In 7 showed that the Enigma cipher procedure then being used (double encipherment of the message setting) was extremely dangerous, because as a result the enemy would be enabled in certain special cases to recover the day key. To do this either a special deciphering machine was required, or a lengthy Hollerith operation which need only be performed once. I cannot remember the details of the method (however, see concluding remark). At that time it appeared doubtful that the Poles had carried out so great a task with their machines. In any case the Enigma cipher procedure was duly altered at the beginning of '40. The whole matter then rested until '43 or '44 when suddenly one day the news came in that there were two Polish officers (Lt. Col and Major?) in a Polish P/W camp in N.W. GERMANY who had held leading positions in the WARSAW Cryptanalytic Bureau.

Doc ID: 6587330

(After the collapse of POLAND they had fled to FRANCE and were taken to a German P/W camp there in 1940). Thereupon Dr. PIETSCH visited both of them; they willingly gave him information, as after so long a period the question of security seemed pointless even from the Polish point of view. They said that the Poles had in fact been reading the German Army Enigma in part already several years before the war. But suddenly some alteration was made by the Germans which made it impossible for the Poles to continue reading the traffic. They could no longer remember the date of this alteration. Above all, it did not as far as I know become clear at the interrogation whether between September '39 and the date when the Germans altered the cipher procedure the cryptanalytic work formerly done in WARSAW was continued on French soil, or whether it ceased completely with the capitulation of POLAND. The officers could give no details of the method used, because as heads of section already before 1939 they probably did not know much about the details of the method, which was certainly a complicated one, and also because of the years which had elapsed since then. I know all this only from a short conversation with Dr. PIETSCH and hence am hazy about the details. Dr. PIETSCH did not know exactly where the name "Fall Wicker" came from; it was taken over from the period before 1940; "Wicher" is supposed to be a Polish word meaning something like "Blitz".

15) What is last known location of the OKW/Chi Cryptanalytic machinery?

The machines were lying in the cellar of the"Hans des Fremdenverkehrs", BERLIN, Potsdamerstr, and were definitely there in the late autumn of 1944 and very probably still there in January 1945. I suspect that the equipment was taken along when the section moved to HALLE.

Concluding remarks on questions 4,16 (What was the C.36 method developed by Dr. von DENFFER? Describe in detail.), 17 (Describe the way in which the omega-squared test was used. How did it differ from the chi-squared test?) and 14.

In these cases complicated methods of decipherment are involved, some of them the result of lengthy scientific work and none of them to be described in a few lines. Many details of them have escaped my memory, partly because it is several years ago when I was occupied with them, partly because of the heavy mental stress imposed on me in the last few months. As I have already told Major BUNDY, I am in a position and am willing to make a scientific study of these and similar problems of cryptanalytic theory. It is obvious that I cannot carry out such scientific work as a prisoner. The uncertainty about the fate of myself and of my family is such a cause of anxiety as to make concentrated mental work inconceivable. Moreover, such scientific work involves certain prerequisites, such as for example access to a scientific library. In this connection I may point out that I and also my fellow-prisoners DETTMANN and SAMSONOV have voluntarily placed out knowledge and ability at the disposal of the USFET Intelligence Service, that we have done our level best to supply detailed and accurate information (several hundred pages of written reports and many hours of oral interrogation).

Doc ID: 6587330

On conclusion of our interrogation in August we were taken to OBER-URSEL and received there treatment such as is normally accorded to criminals. (For example I was four whole weeks, partly in humiliating conditions, in strictest solitary confinement). From OBER-URSEL we went to the PW Camp A 21 at DARMSTADT, where we have been waiting six weeks for the release promised us. It is incomprehensible to us why our voluntary cooperation has only brought us most severe disadvantages (at times humiliating treatment, impossibility of getting in touch with our families by post or any other means, delay in our release), while on the other hand our interrogation officers always led us to believe that we had supplied the USFET Intelligence Service with information of the utmost value.

[Signed] Dr. OTTO BUGGISCH